

**TRANSMITTAL OF INFORMATION DISCLOSURE STATEMENT**

Under 37 CFR 1.97(b), (c), or (d)

Docket No. **2182**SRI/ 4374-2 **#10**In re Application of: **Porras, et al.**Serial No.  
**09/996,154**Filing Date  
**November 28, 2001**

Examiner

Group Art Unit **11-283**Title: **APPLICATION-LAYER ANOMALY AND MISUSE DETECTION****RECEIVED**Address to:  
Commissioner for Patents  
Alexandria, VA 22313-1450**NOV 20 2003**

Technology Center 2100

**37 CFR 1.97(b)**

1. ☒ The Information Disclosure Statement submitted herewith is being filed within three months of the filing of a national application other than a continued prosecution application under 37 CFR 1.53(d); within three months of the date of entry of the national stage as set forth in 37 CFR 1.491 in an international application; before the mailing of a first Office Action on the merits; or before the mailing of a first Office Action after the filing of a request for continued examination under 37 CFR 1.114.

**37 CFR 1.97(c)**

2. ☐ The Information Disclosure Statement submitted herewith is being filed after the period specified in 37 CFR 1.97(b), but prior to the mailing date of a Final Action under 37 CFR 1.113, a Notice of Allowance under 37 CFR 1.311, or an Action that otherwise closes prosecution in the application, and is accompanied by the statement or fee as indicated below.

**37 CFR 1.97(d)**


3. ☐ The Information Disclosure Statement submitted herewith is being filed after the period specified in 37 CFR 1.97(c), but on or before payment of the issue fee and is accompanied by the statement and fee as indicated below.

**Required Statements and/or Fees Under 37 CFR 1.97(c) or (d)**

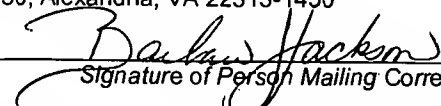
- ☐ Each item of information contained in the accompanying Information Disclosure Statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the Information Disclosure Statement. (37 CFR 1.97(e)(1))
- ☐ No item of information in the accompanying Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned person, after making reasonable inquiry, no item of information contained in the accompanying Information Disclosure Statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the Information Disclosure Statement. (37 CFR 1.97(e)(2))
- ☐ The fee set forth in 37 CFR 1.17(p). Please credit any overpayment or charge any insufficiencies to deposit account number 20-0782.

**37 CFR §1.704(d)**

4. ☐ Each item of information in the accompanying Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart application and this communication was not received by any individual designated in 37 CFR §1.56(c) more than thirty days prior to the filing of the Information Disclosure Statement.

  
Kin-Wah TONG  
Reg. No. 39,400Dated: 11/11/03**Certificate of Mailing by First Class Mail**

I certify that this document is being deposited on 11-12-2003 with the U.S. Postal Service as first class mail under 37 CFR §1.8 and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

  
Signature of Person Mailing Correspondence**Barbara J. Jackson**

Typed or Printed Name of Person Mailing Correspondence

**Moser, Patterson & Sheridan, LLP**  
Attorneys at Law  
595 Shrewsbury Avenue, Suite 100  
Shrewsbury, New Jersey 07702  
732-530-9404

U.S. Department of Commerce, Patent and Trademark Office		Docket No.	Serial No.
(PTO Form 1449 modified)		SRI 4374-2	09/996,154
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>		Applicant Porras, et al.	Confirmation No.: 2117
(Use several sheets if necessary)		Filing Date	Group
Examiner		November 28, 2001	2182

**U.S. Patent Documents**

*Examiner Initial		Document Number	Issue Date	Applicant(s) Name	Class	Subclass	Filing Date If Appropriate
	A1	5,440,723	08/08/1995	Arnold et al.	395	181	
	A2	2003/0145226	07/31/2003	Bruton, III et al.	713	201	01/28/2002
	A3	2003/0172166	09/11/2003	Judge et al.	709	229	03/08/2002
	A4						
	A5						

RECEIVED

NOV 20 2003

**Foreign Patent Documents**

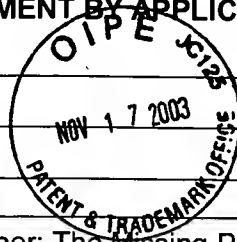
Technology Center 2100

*Examiner Initial		Document Number	Date	Country	Class	Subclass	Translation	
							YES	NO
	B1	03/077071	09/18/2003	WIPO	G06F		<input checked="" type="checkbox"/>	<input type="checkbox"/>
	B2						<input type="checkbox"/>	<input type="checkbox"/>
	B3						<input type="checkbox"/>	<input type="checkbox"/>
	B4						<input type="checkbox"/>	<input type="checkbox"/>

**OTHER ART**

*Examiner Initial		Including Author, Title, Date, Pertinent Pages, Etc.
	C1	Almgren, et al., "A Lightweight Tool for Detecting Web Server Attacks," Network and Distributed Systems Security (NDSS 2000) Symposium Proceedings, 157-170, 2000
	C2	Almgren, et al., "Application-Integrated Data Collection for Security Monitoring," From <i>Recent Advances in Intrusion Detection (RAID 2001)</i> , Springer, Davis, California, October 2001, pg 22-36
	C3	Daniels, et al., "A Network Audit System for Host-Based Intrusion Detection (NASHID) in Linux," 16 <sup>th</sup> Annual Computer Security Application Conference (ACSAC'00) December 11-15, 2000, New Orleans, LA
	C4	Daniels, "Identification of Host Audit Data to Detect Attacks on Low-Level IP Vulnerabilities," J. Computer Security, 7(1): 3-35, 1999
	C5	Dayioglu, "APACHE Intrusion Detection Module," <a href="http://yunus.hacettepe.edu.tr/~burak/mod_id/">http://yunus.hacettepe.edu.tr/~burak/mod_id/</a> , Date Unknown, Downloaded November 10, 2003
	C6	Hollander, Y., "The Future of Web Server Security: Why your Web site is still vulnerable to attack," <a href="http://www.cgisecurity.com/lib/wpfuture.pdf">http://www.cgisecurity.com/lib/wpfuture.pdf</a> , allegedly posted 2000
	C7	Lindqvist, et al., "eXpert-BSM: A Host-based Intrusion Detection Solution for Sun Solaris," Proc. 17 <sup>th</sup> Annual Computer Security Application Conference, pg 240-251, New Orleans, LA, December 10-14, 2001

U.S. Department of Commerce, Patent and Trademark Office		Docket No.	Serial No.
(PTO Form 1449 modified)		SRI 4374-2	09/996,154
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>		Applicant Porras, et al.	Confirmation No.: 2117
(Use several sheets if necessary)		Filing Date	Group
Examiner		November 28, 2001	2182



C8	Munson, et al., "Watcher: The Missing Piece of the Security Puzzle," Proceedings of the 17th Annual Computer Security Applications Conference (ACSAC'01), December 10-14 2001, New Orleans, LA, pp 230-239, IEEE Press.
C9	Porras et al, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," 20 <sup>th</sup> NISSC – October 9, 1997, pg. 353-365.
C10	Tener, "AI and 4GL: Automated Detection and Investigation Tools", Proceedings of the IFIP Sec. '88, Australia, 1989, pp 23-29.

Examiner	Date Considered
----------	-----------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with your communication to applicant.

**RECEIVED**

NOV 20 2003

Technology Center 2100